IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
NORFOLK DIVISION

UNITED STATES OF AMERICA,

v. CRIMINAL NO. 2:16cr43

HUNTER VAUGHAN EURE,

Defendant.

MEMORANDUM OPINION

This matter comes before the Court on two Motions to Suppress filed by Hunter Vaughan Eure ("Defendant"). ECF Nos. 21, 22. On July 5, 2016, the Court held a hearing on these and other motions. Hr'g, ECF No. 44. From the bench the undersigned **DENIED** Defendant's First Motion to Suppress, ECF No. 21, and **DENIED** Defendant's Second Motion to Suppress, ECF No. 22. This memorandum opinion memorializes the reasons for these denials.

I. BACKGROUND

The instant prosecution is the result of an FBI investigation into a website that facilitated the distribution of child pornography. The government seized control of this website and for a brief period of time operated it from a government facility in the Eastern District of Virginia. Both Motions to Suppress seek to exclude all evidence obtained as the result of a search warrant that allowed the government to use the website to remotely search the computers of individuals who logged into the website.

The following summary is provided as way of background. The basic details of the investigation are not in dispute. Most of the information summarized here has been drawn from the warrant application, Appl. for a Search Warrant ("Warrant Appl."), ECF No. 21-1, specifically the affidavit in support of the warrant sworn to by FBI Special Agent Douglas

Macfarlane. Aff. in Supp. of Appl. for Search Warrant ("Macfarlane Aff."), ECF No. 21-2 at 2. Additional details undisputed by the parties in their briefing are included mainly to fill out the narrative. For instance, neither the warrant nor warrant application identify the website and both refer to it simply as "TARGET WEBSITE." See Macfarlane Aff. ¶ 4. As explained in the affidavit in support of the warrant, at the time the warrant application was submitted the website was still active. Id. ¶ 2 n.1. The government was concerned that disclosure of the name of the website in the application would alert potential users of the site to the government's investigation and thus undermine it. Id. The government has ceased operation of the website, and the name of the website has been widely reported.[1] Both parties refer to the website by its name: Playpen.

Playpen operated on the Tor network, which provides more anonymity to its users than the regular Internet.[2] Macfarlane Aff. ¶¶ 7–8. The Tor network was developed by the U.S. Naval Research Laboratory and is now accessible to the general public. Id. ¶ 7. Users of the Tor network must download special software that lets them access the network. Id. Typically, when an individual visits a website, the website is able to determine the individual's Internet Protocol ("IP") address. See id. ¶ 8. An individual's IP address is associated with a particular Internet Service Provider ("ISP") and particular ISP customer. Id. ¶ 35. Because internet access is typically purchased for a single location, an IP address may be used by law enforcement to determine the home or business address of an internet user. See id. When a user accesses the Tor network, communications from that user are routed through a system of network computers that are run by volunteers around the world. Id. ¶ 8. When a user connects to a website, the only IP address that the website "sees" is the IP address of the last computer through which the user's

[1] See e.g., Joseph Cox, The FBI's 'Unprecedented' Hacking Campaign Targeted Over a Thousand Computers, Motherboard, Jan. 5, 2016, http://motherboard.vice.com/read/the-fbis-unprecedented-hacking-campaign-targeted-over-a-thousand-computers.

[2] The Tor network is also known as "The Onion Router." Macfarlane Aff. ¶ 7. More information about it may be found on its website: www.torproject.org.

communications were routed. Id. This final relay is called an exit node. Id. Because there is no practical way to trace a user's communications from the exit node back to the user's computer, users of the Tor network are effectively anonymous to the websites they visit. Id.

The Tor network also provides anonymity to individuals who run websites or forums on it. Id. ¶ 9. Websites may be set up on the Tor network as "hidden services." Id. A hidden service may only be accessed through the Tor network. Id. A hidden service functions much like a regular website except that its IP address is hidden. Id. The IP address is replaced with a Tor-based address which consists of a series of alphanumeric characters followed by ".onion." Id. There is no way to look up the IP address of the computer hosting a hidden service. Id.

A user of the Tor network cannot simply perform a search to find a hidden service that may interest the user. Id. ¶ 10. In order to access a hidden service a user must know the Tor-based address of the hidden service. Id. As a result, a user cannot simply stumble onto a hidden service. Id. The user may obtain the address from postings on the Internet or by communications with other users of the Tor network. Id. One hidden service may also link to another. See id. Playpen was a hidden service contained on the Tor network, and it had been linked to by another hidden service that was dedicated to child pornography. Id.

Of importance to the First Motion to Suppress is the homepage of the Playpen site. See Def.'s First Mot. to Suppress ("First Mot."), ECF No. 21 at 2–3. In the warrant application, the homepage is said to contain "images of prepubescent females partially clothed and whose legs are spread." Macfarlane Aff. ¶ 12. A screenshot of this version of the homepage has been attached to the briefing. ECF No. 27-4. There appears to have just been two photographs on the homepage. The images show two young girls in the attire and pose described. Id. The images of these children appear at the top of the homepage and flank a large image of the site's name,

Playpen. Id. In their briefing, the parties describe the combination of these images and the site name as the site logo. Although these images were at an earlier point on the homepage, the parties agree that at the time the warrant was signed, on February 20, 2015 at 11:45 a.m., a different logo confronted users to the site. First Mot. at 8–9; Gov't's Resp. to Def.'s First Mot. to Suppress ("Gov't's Resp. to First Mot."), ECF No. 27 at 14–15. A screenshot of this version of the homepage has also been included in the briefing. ECF No. 17-5. There is an image of a young girl with her legs crossed, reclined on a chair, wearing stockings that stop at her upper thigh and a short dress or top that exposes the portion of her upper thigh not covered by the stockings. Id. Her image is to the left of the site name in this version of the site logo. Id.

The government claims that the images must have changed shortly before the warrant was signed. Gov't's Resp. to First Mot. at 14–15. In the affidavit in support of the warrant, Special Agent Macfarlane recounts that FBI agents monitored the Playpen website from September 16, 2014 to February 3, 2015. Macfarlane Aff. ¶ 11. The screenshot of the homepage that was included in the government's brief and contains the images of the two young girls was taken on February 3, 2015. ECF No. 27-4. The date is visible in the lower right corner of the screen. Id. The affidavit further states that sometime between February 3, 2015 and February 18, 2015, the Tor address of the site was changed. Macfarlane Aff. ¶ 11 n.3. Special Agent Macfarlane states in his affidavit that after the address change he "accessed the TARGET WEBSITE in an undercover capacity at its new URL, and determined that its content had not changed." Id. In its briefing the government asserts that this statement confirms that the homepage of Playpen was as described in the warrant application on February 18, 2015, two days before the warrant was sworn and signed. Gov't's Resp. to First Mot. at 14–15.

The homepage also provided users with instructions on how to join and then log into the

site. Macfarlane Aff. ¶ 12. Users had to register with the site before going any further into the site. Id. Users were instructed to enter a phony email address and to create a login name and password. Id. ¶ 13. The instructions also informed users that the owners of the site and staff were unable to determine the true identity of users and that the website could not see the IP addresses of users. Id.

Once registered and logged into the site users had access to numerous sections, forums, and sub-forums where they could upload material and view material uploaded by others. Id. ¶ 14. For instance under the heading "Playpen Chan"[3] are four subcategories: "Jailbait – Boy," "Jailbait – Girl," "Preteen – Boy," and "Preteen – Girl." Id. Special Agent Macfarlane, based on his training and experience, explains that "jailbait" refers to underage but post-pubescent minors. Id. ¶ 14 n.4. Other forum and sub-forum categories on the site include "Jailbait videos," "Family Playpen – Incest," "Toddlers," and "Bondage." Id. ¶ 14. Not surprisingly, a review of the contents of these forums revealed that the majority of content was child pornography. Id. ¶ 18. The warrant application has several specific examples of the reprehensible material contained on the site. Id. ¶¶ 18, 23–25. Additionally, there was a section of the site that allowed members of the site to exchange usernames on a Tor-based instant messaging service known to law enforcement to be "used by subjects engaged in the online sexual exploitation of children." Id. ¶ 15.

In December of 2014, a foreign law enforcement agency informed the FBI that it suspected that a United States-based IP address was the IP address of Playpen. Id. ¶ 28. In January 2015, after obtaining a search warrant, the FBI seized the IP address and copied the contents of the website. Id. ¶ 28. On February 19, 2015 the FBI arrested the individual suspected

[3] "Chan" is a common postscript for online bulletin boards where users may post pictures and messages. See Nick Bilton, One on One: Christopher Poole, Founder of 4chan, Bits Blog, New York Times, Mar. 19, 2010, http://bits.blogs.nytimes.com/2010/03/19/one-on-one-christopher-poole-founder-of-4chan/.

of administering Playpen. Id. ¶ 30.

The FBI desired to continue to operate Playpen for a limited time so as to identify individuals who logged into the site and who were likely to possess, distribute, or produce child pornography. Id. ¶ 30. The FBI would operate the site from a location in the Eastern District of Virginia. Id. ¶ 33. As mentioned above, normally a website administrator is able to determine the IP addresses of those individuals that visit the site. However, on the Tor network the website administrator is only able to determine the IP address of the exit node, which it not the IP-address of the visitor to the website. To determine the IP addresses of individuals who logged into Playpen, the FBI sought a warrant from a magistrate judge in the Eastern District of Virginia, Alexandria Division that would allow it to deploy a Network Investigative Technique ("NIT"). Id. ¶ 31.

According to the FBI in the warrant application, when an individual visits a website the website sends "content" to the individual. Id. ¶ 33. This content is downloaded by the individual's computer and used to display the webpage on the computer. Id. A NIT "augments" the content with additional instructions. Id. The NIT deployed in the instant case instructed the computers of those individuals who logged into Playpen to send to a computer "controlled by or known to the government" certain information. Id. The information that the NIT would instruct the computers to send is described in an attachment to the warrant application. Attach. B, Warrant Appl., ECF No. 21-1 at 3. The NIT extracted from any "activating computer"—that is, a computer that logged into Playpen using a username and password—(1) the IP address of the computer and the date and time this information is determined, (2) a unique identifier that distinguishes the data from this activating computer from that of others, (3) the type of operating system used by the computer, (4) information about whether the NIT has already been sent to the

computer, (5) the computer's Host Name, (6) the computer's operating system user name, and (7) the computer's media access control ("MAC") address. Id.

On February 20, 2016 at 11:45 a.m., Magistrate Judge Theresa Carroll Buchanan of the United States District Court for the Eastern District of Virginia, Alexandria Division, issued the requested warrant. Warrant Appl., ECF No. 21-1 at 1. The warrant permitted the FBI to run Playpen from a location in the Eastern District of Virginia for thirty (30) days and to deploy a NIT from the website. Id. at 2–3. The NIT would instruct any computer that logged into Playpen with a username and password to send the just described information. Id.

According to the briefing of Defendant, on or about February 22, 2015, the Playpen website sent the NIT to Defendant's computer. First Mot. at 10. Using the information obtained through the NIT, the FBI issued an administrative subpoena to Verizon, Defendant's ISP. Id. Verizon then provided the FBI with Defendant's subscriber information, name, and address. Id. On January 4, 2016, Magistrate Judge Lawrence R. Leonard issued a warrant to search Defendant's home. Id. On January 20, 2016, the FBI and other law enforcement agents searched Defendant's home pursuant to this warrant. Id. The agents seized a computer and thumb drive. Id.

According to the government, Defendant was not present in his home during the search. Gov't's Resp. to First Mot. at 7. FBI agents interviewed him at his work. Id. Defendant told agents that he accessed and downloaded images of minors engaging in sexually explicit content. Id. He told agents that he viewed child pornography on a daily basis. Id.

On March 24, 2016, Defendant was indicted on three counts of Receipt of Images of Minors Engaging in Sexually Explicit Conduct, in violation of 18 U.S.C. § 2252(a)(2), and one count of Possession of Images of Minors Engaging in Sexually Explicit Conduct, in violation of

18 U.S.C. § 2252(a)(4)(B). Indictment, ECF No. 14. On May 16, 2016, Defendant filed his First Motion to Suppress, ECF No. 21, and his Second Motion to Suppress, ECF No. 22. The government responded to both motions on May 31, 2016. ECF Nos. 27, 28. Defendant replied to both responses on June 3, 2016. ECF No. 29, 30. The Court allowed argument on both Motions to Suppress during a hearing held on July 5, 2016. Hr'g, ECF No. 44. The Court also heard argument on Defendant's pending Motion to Compel Discovery.[4] See Mot. to Compel Disc., ECF No. 23. Two witnesses testified at the hearing. Defendant called Dr. Christopher Soghoian, a technologist. Hr'g, ECF No. 44. The government called FBI Special Agent Daniel Alfin. Id. At the conclusion of the hearing the undersigned denied both Motions to Suppress from the bench. Id.

II. LEGAL PRINCIPLES AND ANALYSIS

The exact issues raised by the instant motions to suppress were also raised by the defendant in United States v. Gerald Andrew Darby, 2:16cr36, another case pending before the undersigned. The Court denied both Motions to Suppress in Darby and issued a written opinion justifying its denial. United States v. Darby, No. 2:16cr36, 2016 WL 3189703 (E.D. Va. June 3, 2016). The Court explained why the issuance of the NIT warrant did not violate either the Fourth Amendment or Federal Rule of Criminal Procedure Rule 41(b). Although the factual record in the instant case has been supplemented by Defendant, the reasons the Court gave in Darby for denying the Motions to Suppress apply with equal force here. Accordingly, the Court hereby incorporates its opinion in Darby. The undersigned writes further to emphasize that suppression is an extraordinary remedy and would not be appropriate in the instant case even if, as Defendant maintains, there were a violation of the Fourth Amendment or of Rule 41(b).

[4] The hearing also concerned a similar Motion to Compel Discovery filed in another case pending before the undersigned, United States v. Gerald Andrew Darby, 2:16cr36. The defendant in that case was also located by the government using the NIT deployed through the Playpen website.

A. THE SCOPE OF THE EXCLUSIONARY RULE

As the Supreme Court has emphasized again and again in recent years, the suppression of evidence is not the appropriate remedy for every violation of the Fourth Amendment. Herring v. United States, 555 U.S. 135, 140 (2009) (citing Illinois v. Gates, 462 U.S. 213, 223 (1983)). "Each time the exclusionary rule is applied it exacts a substantial social cost for the vindication of Fourth Amendment rights." Rakas v. Illinois, 439 U.S. 128, 137 (1978). Accordingly, the exclusionary rule is the "last resort" for the courts and should not be the "first impulse." Utah v. Strieff, 136 S.Ct. 2056, 2061 (2016) (quoting Hudson v. Michigan, 547 U.S. 586, 591 (2006)). Suppression is only appropriate when the benefits of suppression outweigh its costs. Herring, 555 U.S. at 141 (citing United States v. Leon, 468 U.S. 897, 910 (1984)).

The goal of the exclusionary rule, its benefit, is that it may deter police misconduct. Id. (citing Leon, 468 U.S. at 909). The extent of deterrence "varies with the culpability of the law enforcement conduct." Id. at 143. There is a greater need to deter more culpable conduct and the more culpable the police misconduct, the greater deterrent effect of suppression—it is impossible to deter innocent conduct. See id. at 144. Against the need and effect of deterrence, a district court must consider the "substantial social costs" of suppression. Id. at 141 (quoting Illinois v. Krull, 480 U.S. 340, 352–353 (1987)). "The principal cost of applying the rule is, of course, letting guilty and possibly dangerous defendants go free—something that 'offends basic concepts of the criminal justice system.'" Id. (quoting Leon, 468 U.S. at 908).

To summarize all of the above in test form, the Supreme Court has instructed district courts to consider whether the conduct of law enforcement was: (1) "sufficiently deliberate [such] that exclusion can meaningfully deter it," and (2) "sufficiently culpable that such deterrence is worth the price paid by the justice system." Id. at 144. This analysis must be performed in every case where suppression is sought. See Strieff, 136 S.Ct. at 2061 ("[T]he

significant costs of this rule have led us to deem it applicable only where its deterrence benefits outweigh its substantial social costs." (emphasis added) (internal quotations and citation omitted)). Although the Supreme Court has consistently referred to exceptions to the exclusionary rule, Strieff, 136 S.Ct. at 2061, its recent Fourth Amendment jurisprudence, especially the opinion in Herring, suggests that suppression is the exception.[5]

B. FIRST MOTION TO SUPPRESS

In his First Motion to Suppress Defendant raises several related grounds for suppressing the fruits of the search executed pursuant to the NIT warrant. First, he argues that the warrant was not supported by probable cause. First Mot. at 2. Second, he argues the FBI, either intentionally or recklessly, misled the warrant issuing court with its description of Playpen's homepage. Id. at 2–3. He demands a Franks hearing on this issue. Id.; see Franks v. Delaware, 438 U.S. 154 (1978). Third, he argues that the NIT warrant was an anticipatory warrant and that the triggering event establishing probable cause did not occur. First Mot. at 3.

As this Court explained in Darby, each of these arguments is premised on the contention, rejected in Darby, that there was not probable cause to search the computers of those users who logged into Playpen after the images on the homepage were changed. See Darby, 2016 WL 3189703, at *7–10. The warrant application described the homepage as containing, to the left and right of the site logo, two young female children in their underwear with their legs spread. At the time the warrant application was submitted and when the warrant was executed there was a single image beside the site logo of a slightly older child whose legs were crossed and who was

[5] Defendant's recitation of language from Terry v. Ohio about the importance of the exclusionary rule is a misstatement of current Supreme Court doctrine. See, e.g., Def.'s Reply to Gov't's Resp. to First Mot. to Suppress ("Reply to Gov't's Resp. to First Mot."), ECF No. 30 at 15 (quoting Terry). For instance, the Supreme Court in Herring is explicit in stating that the only purpose of the exclusionary rule is the deterrence of police misconduct. 555 U.S. at 141. Yet, Defendant, quoting Terry, asserts that suppression serves "the imperative of judicial integrity." Reply to Gov't's Resp. to First Mot. at 15. In Herring, the Supreme Court comes close to saying the opposite of this when it writes that to let criminals go free because of the suppression of evidence "offends basic concepts of the criminal justice system." Herring, 555 U.S. at 141 (quoting Leon, 468 U.S. at 908).

wearing stockings and a short dress or top. In Darby, the undersigned explained why there was probable cause to search the computers of those who registered and logged into the website even after the change to the website. Darby, 2016 WL 3189703, at *7–8. However, even assuming that there was not probable cause to search, suppression would not be appropriate.

It is well-established that "[w]hen police act under a warrant that is invalid for lack of probable cause, the exclusionary rule does not apply if the police acted 'in objectively reasonable reliance' on the subsequently invalidated search warrant." Herring, 555 U.S. at 142 (quoting Leon, 468 U.S. at 922). Defendant argues that this "exception," typically referred to as the Leon "good faith exception," does not apply because the FBI misled the magistrate judge with information it knew to be false and because the good faith exception does not apply if a law enforcement officer wrongly concludes that the triggering event of an anticipatory warrant has occurred. See Reply to Gov't's Resp. to First Mot. at 15–17.

In support of his first argument, Defendant cites to the exceptions identified by the Supreme Court in Leon to the good faith exception applied in that case. The good faith exception does not apply: (1) "if the magistrate or judge in issuing a warrant was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth;" (2) "if the issuing magistrate wholly abandoned his judicial role;" (3) "if the affidavit supporting the warrant is so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable;" or (4) "if under the circumstances of the case the warrant is so facially deficient . . . that the executing officers cannot reasonably presume it to be valid." United States v. Doyle, 650 F.3d 460, 467 (4th Cir. 2011) (internal quotations omitted) (quoting United States v. DeQuasie, 373 F.3d 509, 519–20 (4th Cir. 2004). After Herring, it is probably best to view these exceptions to the good faith exception as

distillations of the cost-benefit analysis mandated in Herring. Upon close analysis, all of the factors inquire into whether there was any wrongdoing by law enforcement officers in obtaining and executing the warrant. The first exception does this explicitly. The other three require an inquiry into the extent of the deficiency of the warrant application approved by the magistrate. Of course, law enforcement officers must submit the warrant application to the magistrate and are responsible for any gross deficiencies.

In this case, Defendant has presented evidence that at least one FBI agent reviewed the website after it had changed and before the warrant application was submitted to the magistrate judge. As recounted in the warrant application, the FBI seized control of the server that hosted the Playpen website sometime in January 2015. Macfarlane Aff. ¶ 28. On February 19, 2016, the FBI executed a search warrant at the home of the individual suspected of administrating Playpen. Id. ¶ 30. The next day, on February 20, 2016, the FBI applied for and was granted the NIT warrant. As described above, Agent Macfarlane, who submitted the affidavit in support of the warrant, reviewed the website on February 18, 2016 and did not notice any changes to the site. See id. ¶ 11 n. 3. It is the government's position that Agent Macfarlane's sworn statement that the website on February 18, 2016 looked the same as it did on February 3, 2016 is evidence that the website must have changed sometime after February 18.[6] Gov't's Resp. to First Mot. at 14–15. In a hearing held in another proceeding, Special Agent Daniel Alfin, who testified in this Court's hearing on the instant motions, testified that he viewed the website as it appeared on February 19 and on the morning of February 20, before the warrant application was submitted. Test. of Special Agent Daniel Alfin, Hr'g Tr. at 89:15-18 (Jan. 22, 2016), United States v. Michaud, No. 15-5351 (W.D. Wash. Jan. 26, 2016). He conceded that the warrant application

[6] As noted above, a screenshot taken on February 3 confirms that on February 3 the website looked as it is described in the warrant application. ECF No. 27-4.

"reflected a specific period of review, and it was not updated to include my observations from the night of February 19th and morning of February 20th." Id. He also testified that "I would have clearly seen the website and would have seen the new logo, [but] it did not jump out to me as a significant change to the website or a material change to the website." Id. at 84:12-15. Similarly, in testimony before the Honorable Judge Morgan,[7] the undersigned's colleague in the Norfolk Division of the United States District Court for the Eastern District of Virginia, Special Agent Alfin testified that "I saw [the new logo], but I did not notice it because it was an insignificant and minor change to the Web site." Test. of Special Agent Alfin, Hr'g Tr. at 10:24-25 (May 19, 2016), United States v. Edward Joseph Matish, No. 4:16cr16, ECF No. 61 (E.D.Va. May 24, 2016), docketed in the instant case at ECF No. 29-1. When asked to confirm that he had seen the new logo, Special Agent Alfin stated that "yes, I did see it, and, as I stated previously, it went unobserved by me because it was an insignificant change to the Web site." Id. at 11:5-7.

From the testimony cited above, it is certain that, at the very least, Special Agent Alfin saw the changed website. His testimony as to whether he noticed the change might appear at first glance to be inconsistent. In his testimony in the Western District of Washington, he claims to have seen the new logo but that the change did not "jump out" to him as "significant" or "material" while before Judge Morgan he claims that he did not "notice" the change because it was "insignificant" and "minor." To see something is not necessarily to have noticed it. To say that the change did not "jump out" may be another way of saying that he did not notice the change. There is nothing in the record indicating whether Special Agent Alfin told Special Agent Macfarlane, who signed the affidavit in support of the warrant, about any changes to the website.

[7] In United States v. Matish, No. 4:16CR16, 2016 WL 3545776 (E.D. Va. June 23, 2016), Judge Morgan has issued an excellent opinion on the issues raised by the Motions to Suppress filed in this case. Although the undersigned does not agree with every aspect of Judge Morgan's opinion, the undersigned recommends reading the opinion for its compelling treatment of the important issues raised by the government's use of the NIT warrant.

If Special Agent Alfin had not noticed the change, he could not have told Special Agent Macfarlane, and if he did notice, he should have told Special Agent Macfarlane. But whatever Special Agent Alfin's cognizance of the change to the website's logo, the FBI filed a false warrant application even though its agent had seen the changed website and could have reviewed it more thoroughly to ensure that it matched the description in the warrant application. As the Court explained in Darby, the changes to the website logo were immaterial and there was probable cause to search anyone who visited and then logged into the changed homepage. Darby, 2016 WL 3189703, at *7–8. However, Defendant is correct in arguing that it is for the magistrate judge to decide whether any changes to the website were material. The FBI should have done more to ensure that its description of the website in the warrant application was correct.

Nonetheless, the FBI agents' behavior in failing to submit an accurate warrant application does not rise to a level of culpability that would justify suppression if this Court is wrong in its determination that the warrant was supported by probable cause. The FBI agents were operating under severe time constraints. They raided the home of the individual that administered Playpen on February 19, 2016 and submitted the warrant application the next day. The government desired to deploy the NIT as soon as possible so that it could identify as many visitors to Playpen as possible. See Gov't's Resp. to Def.'s Second Mot. to Suppress ("Gov't's Resp. to Second Mot."), ECF No. 28 at 20. Because of the security features of the Tor browser, without the NIT the government would be unable to identify those users even when it was administering the website. Macfarlane Aff. ¶ 29. Any delay in receiving the warrant provided a window for individuals to visit Playpen and download child pornography without detection. It is well established that exigent circumstances may make a warrantless search reasonable within the meaning of the Fourth Amendment. Kentucky v. King, 563 U.S. 452, 460 (2011). In Darby, this

Court explained that the fact that the government was able to obtain a warrant somewhat undercuts its argument that exigent circumstances justified deploying the NIT without a warrant. Darby, 2016 WL 3189703 at *13 n.8. However, although circumstances might not have justified a warrantless search, they reduce the culpability of the FBI agents in failing to correct the warrant application on account of a minor change to the homepage that occurred within two days of the submission of the application.

Defendant also argues that the good faith exception should not apply because it is inapplicable when a triggering event in an anticipatory warrant does not occur. Reply to Gov't's Resp. to First Mot. at 16; see United States v. Ricciardelli, 998 F.2d 8, 17 n.10 (1st Cir. 1993) ("[I]f a situation arises in which officers wrongly conclude that the triggering event needed to animate an anticipatory warrant has occurred, and proceed to execute a full search in the face of this mistake, we would not review that mistake under Leon's good faith standard."). Although Defendant relies upon pre-Herring case law in support of this position, Defendant's reasoning would seem to survive the Supreme Court's refocusing of the exclusionary rule in Herring. Herring instructs this Court to assess the culpability of law enforcement in any alleged Fourth Amendment violation. If an event needed to trigger an anticipatory warrant does not occur and yet law enforcement officers execute a search anyway, the officers have failed to follow the parameters of the warrant and may have acted culpably in doing so.

The problem with Defendant's position is that he mischaracterizes the triggering event of the warrant. Defendant claims that the warrant could only be executed after an individual registered with Playpen and then logged into the site when the site homepage was as described in the warrant application. First Mot. at 28. However, as explained in Darby, Defendant mischaracterizes the triggering event of the warrant. Darby, 2016 WL 3189703, at *9. The

triggering event was simply logging into the Playpen website. Id. It was that event that established probable cause to search Defendant's computer. Id. Defendant's characterization attempts to transform a problem in the application for the warrant into a problem in the execution of the warrant. The FBI agents may have submitted, under very real time pressures, an inaccurate warrant application. However, once the warrant was obtained, the agents acted within the parameters of the warrant. The FBI only deployed the NIT against the computers of those individuals who logged into Playpen. Accordingly, there was no wrongdoing in the execution of the warrant that would justify suppression.

In sum, none of the Fourth Amendment violations alleged in Defendant's First Motion to Suppress would justify suppression even if these violations had occurred. Although the FBI agents in this case submitted an inaccurate warrant application, their culpability in doing so is reduced because of the need to obtain the warrant quickly. Once obtained, the agents executed the warrant according to its parameters.

C. SECOND MOTION TO SUPPRESS

In his Second Motion to Suppress, Defendant argues that the magistrate judge lacked jurisdiction under the Federal Magistrates Act, which incorporates Federal Rule of Criminal Procedure 41(b), to issue the NIT warrant. Def.'s Second Mot. to Suppress ("Second Mot.), ECF No. 22 at 2. Because the magistrate judge lacked jurisdiction to issue the warrant, the warrant was issued without lawful authority and void at the outset. Id. If the warrant was void, the search of Defendant's computer was performed without a valid warrant in violation of the Fourth Amendment. Because of this alleged constitutional violation Defendant seeks to suppress all fruits of the search performed under the NIT warrant. In the alternative, Defendant argues that the fruits of the NIT warrant should be suppressed because he was prejudiced by the alleged violation of Rule 41(b) and because the government's violation of the rule was deliberate. Id.

Each of these grounds for suppression depends upon a simple contention: nothing in Rule 41(b) allowed the magistrate judge to issue the NIT warrant. The magistrate judge could not issue the NIT warrant, according to Defendant, because the warrant allowed the government to perform searches outside of the Eastern District of Virginia and magistrate judges may only authorize searches outside of their judicial districts in limited circumstances.

This Court explained in Darby why Rule 41(b) allowed the magistrate judge to issue the NIT warrant. Darby, 2016 WL 3189703, at *11–12. However, even if Rule 41(b) did not allow the magistrate judge to issue the NIT warrant, suppression would not be justified because the actions of the law enforcement officers in this case were not sufficiently culpable.

Defendant argues that no inquiry into the culpability of law enforcement is necessary because of the nature of the violations of the Fourth Amendment and the Federal Rules of Criminal Procedure that are alleged in the Second Motion to Suppress. Second Mot. at 10–12. Defendant says that the Leon good faith exception does not apply when a warrant is void because a magistrate judge lacked the jurisdiction to issue it. Id. at 10 (citing United States v. Levin, No. CR 15-10271-WGY, 2016 WL 2596010, at *10 (D. Mass. May 5, 2016); Com. v. Shelton, 766 S.W.2d 628, 629–30 (Ky. 1989). Certainly it is true that the rule announced in Leon—that "[w]hen police act under a warrant that is invalid for lack of probable cause, the exclusionary rule does not apply if the police acted 'in objectively reasonable reliance' on the subsequently invalidated search warrant," Herring, 555 U.S. at 142 (quoting Leon, 468 U.S. at 922)—would not seem to apply when the problem with the warrant was something other than a lack of probable cause. However, the rule that the Supreme Court articulated in Herring is broader than the good faith exception applied in Leon. Herring says that the exclusionary rule should only be applied when the actions of law enforcement are so culpable that exclusion can achieve

meaningful deterrence that is worth the price paid by the justice system in suppressing evidence. This is true when a defendant alleges that his constitutional rights have been violated; it must also be true when he alleges merely that the Federal Rules of Criminal Procedure were not followed.

Defendant goes on to argue that "ample evidence points to an intentional and deliberate violation of Rule 41(b). Second Mot. at 11. Because the "exclusionary rule was crafted to curb police rather than judicial misconduct," Herring, 555 U.S. at 142 (citing Arizona v. Evans, 514 U.S. 1, 15 (1995)), the relevant inquiry is whether law enforcement officers intentionally violated Rule 41(b). It is of no consequence whether the magistrate judge knew or should have known that the NIT warrant exceeded her jurisdiction. Defendant argues that the "government" knew that the NIT warrant exceeded the magistrate judge's jurisdiction because the Department of Justice ("DOJ") had been seeking to amend Rule 41(b) to explicitly authorize this type of warrant.[8] However, the question is not what the government collectively knew. The question is what the individual law enforcement officers that submitted the warrant in this case knew. Defendant seeks to attribute to the FBI agents that sought the warrant the legal expertise of the DOJ lawyers but nothing indicates that these agents knew that the warrant might violate Rule 41(b). It is somewhat hard to understand why they would have even submitted the warrant if they thought it exceeded the magistrate judge's jurisdiction. If they were so inclined to flout the Federal Rules of Criminal Procedure, they might have forgone seeking the warrant in the first place.

It was quite logical for the FBI agents to seek this warrant in the Eastern District of

[8] In its briefing the government notes that the Supreme Court has authorized an amendment to Rule 41(b)—to be effective December 1, 2016 absent action from Congress—that explicitly authorizes warrants like the NIT warrant to be issued by magistrate judges whose districts have a connection with the criminal activity being investigated. Gov't's Resp. to Second Mot. at 12 n.3.

Virginia. Because the FBI planned to run the website from a server located in the district there was no district in the country that had a stronger connection to the proposed search. Even if the FBI agents had some indication that the warrant might exceed the jurisdiction of the magistrate judge, there were credible arguments that the current rule allowed this warrant. Just as under the good faith rule of Leon, law enforcement may rely on a magistrate judge's determination that a warrant was supported by probable cause, the agents in this case could rely on the magistrate judge's determination that she had authority to issue the warrant. Nothing in the record indicates that the agents deliberately violated Rule 41(b). Rather, the record indicates that agents sought to comply with the Fourth Amendment's requirement that searches and seizures be reasonable. They gathered evidence over an extended period and filed a detailed affidavit with a federal magistrate judge in the federal judicial district that had the closest connection to the search to be executed. Because the law enforcement officers who applied for the warrant did nothing culpable, none of the allegations in the Second Motion to Suppress, even if true, would justify suppression.

III. CONCLUSION

In Darby this Court explained that the searches and seizures perform pursuant to the NIT warrant did not violate the Fourth Amendment or Rule 41(b). The Court adopts the reasoning in Darby in this case. Additionally, as explained in the above opinion, even if there were a violation of the Fourth Amendment or of Rule 41(b), suppression is not appropriate. Accordingly, the Court has **DENIED** Defendant's First Motion to Suppress, ECF No. 21, and **DENIED** Defendant's Second Motion to Suppress, ECF No. 22.

The Clerk is **DIRECTED** to forward a copy of this Order to all counsel of record.

IT IS SO ORDERED.

/s/
Robert G. Doumar
Senior United States District Judge

UNITED STATES DISTRICT JUDGE

Norfolk, VA
July 28, 2016